NTT DATA
Trusted Global Innovator

Quarterly Report on Global Security Trends

1st Quarter of 2019

NTT DATA
Trusted Global Innovator

Table of Contents

1. Executive Summary

In this report, NTTDATA-CERT surveys and analyzes quarterly global trends from its own perspective based on cybersecurity-related information collected in the survey/analysis period.

Domain Hijacking

An incident in which the official website of a well-known anime drew traffic to a suspicious website through 'domain hijacking,' where the attacker hijacks the domain, drew a lot of attention from the media. As opposed to conventional methods, the incident was notable in that the attacker exploited domain transfer procedures only adopted by JP domains.

Continued web skimming incidents reported

Continued from the fourth quarter of FY2018, there were many web skimming incidents reported, where vulnerable EC sites were exploited and payment information stolen. The risks of EC stores being attacked are rising in light of the increase in types of EC platforms that may be targeted.

BlueKeep | Vulnerabilities in Windows Remote Desktop Services

Regarding vulnerability-related topics, Windows Remote Desktop Services' vulnerabilities announced by Microsoft as potentially resulting in WannaCry-like outbreaks garnered significant coverage. Also referred to as 'BlueKeep' vulnerability, many organizations issued alerts on this security flaw. Microsoft took exceptional measures and released patches for unsupported Windows versions as well.

Outlook

Like the first quarter, the second quarter of FY2019 also expects to see an increase in cyberattacks that directly result in financial damage. Web skimming incidents that continue from the fourth quarter of FY2018 and the first quarter of FY2019 are predicted as well.
The ransomware attacks that hit multiple cities across the US are speculated to have targeted cities with insufficient security measures. The attacks may also spread to cities in other countries.

2. Featured Topics

2.1. Domain Hijacking

Domain hijacking is the act of changing the registration of a domain name by an attacker who doesn't have administrative rights through unauthorized access. After a successful hijacking, the hijacker uses the domain name for command-and-control (C&C) servers, malware distribution centers, phishing sites and other malicious servers. The attacker can have users accessing the hijacked domain download malware or fool users into entering login information on phishing sites.
The following are the three best-known tactics used by domain hijackers: [1]

1. The attacker poses as the domain registrant or administrator to change the domain information registered on the registry (domain name registrar)[1]
2. The attacker exploits vulnerabilities in the authoritative name server to manipulate domain information by gaining unauthorized access to the authoritative name server or submitting and registering fake domain information
3. The attacker exploits vulnerabilities in DNS protocols to send rogue domain data to a cache DNS server to have false domain information cached (DNS cache poisoning)

Nonetheless, the domain hijacking incidents that became news during the first quarter of 2019 differed from these popular methods and instead exploited the domain name transfer procedure between registrars[2] and rewrote the domain information on the registry. Table 1 lists domain hijacking incidents that used this method.

[1] A company that maintains and manages all registered domain information on a database by top-level domain (TLD) [105]. Each top-level is managed by one registry. For example, ".com/.net" is managed by VeriSign and ".jp" is managed by JPRS.

[2] A company designated to database a registry based on the registrant's domain information application [106]. A registrar must be accredited by the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit organization that manages internet resources, including IP addresses and domain names.

Table 1: Domain hijacking cases that exploited transfer procedures

No	Date	Domain attacked	Summary
1	Sept 2018	amusecraft.jp	The domain name of the game software development division operated by game producer SOFTPAL was hijacked. The compromised website stated the domain was transferred to a third party [2] [3].
2	Feb 2019	syrup-soft.jp	The domain name of game producer Klein was hijacked, and the compromised website announced the company's dissolution [4] [5].
3	Feb 2019	sukumizu.jp	The domain name for the website of Suruga Denryoku, a fan circle, was hijacked [6].
4	Apr 2019	lovelive-anime.jp	The domain name for the official website of the anime 'Love Live!' was hijacked. A message stating "We now own Love Live!" was displayed on the compromised website [7] [8].

The general-use JP domain name ending with ".jp" were overwritten for all cases listed in Table 1. Cases 1 and 4 are believed to have been attacked by exploiting the characteristic procedure of transferring general-use JP domain names, given messages were posted on the top pages of their domain names after the domain hijacking (See Figure 1).

Before the domain name was hijacked.
Displayed by Official Web Server.

After a domain is hijacked.
Displayed by another server.

Figure 1: Before and after the Love Live! Official website's domain hijacking

The following steps and Figure 2 explain how the domains were hijacked:

1. The attacker applies for a transfer of the targeted JP domain name to Registrar A that they use
2. After accepting the application, Registrar A applies for a change of the domain name's designated operator to Japan Registry Services Co., Ltd. (JPRS[3]), the registry for JP domains
3. JPRS requests confirmation for approval of the domain name transfer to Registrar B in which the domain registrant will be using
4. Registrar B or the domain name registrant whom Registrar B requests confirmation of approval for transfer does not respond to the request for more than 10 days or approves the transfer by error
5. JPRS approves the transfer and the domain name is transferred to the attacker. The attacker succeeds in domain hijacking.

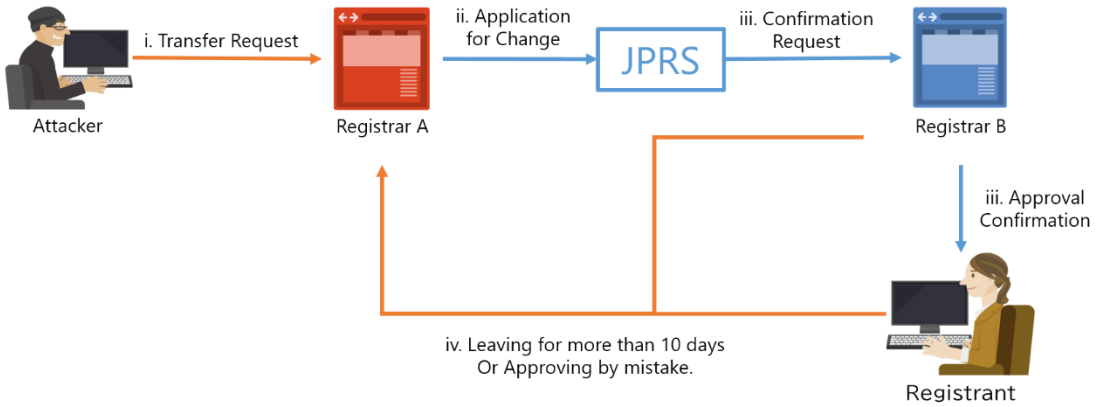


Figure 2: How a domain name is hijacked through exploiting the transfer procedure (Prepared by NTTDATA-CERT)

[3] Japan Registry Services Co., Ltd. Registers and manages JP domain names and operates the JP DNS.

The fact that applications for transfers are automatically approved when the request for confirmation of transfer is not answered for more than 10 days in this JP domain transfer procedure exposes a serious flaw. This rule for automatic approval is stipulated as below in Clause 2, Article 11 of JPRS's "Rules on the Handling of Registration Applications, etc., for General-Use JP Domains." [9].

> *In the event JPRS requests confirmation of the registrant's intent to the designated operator and the said operator does not reply regarding the registrant's intent within 10 days after the request was issued, JPRS shall deem the designated operator has confirmed the registrant's intent as affirmative.*

As indicated above, the rule is an agreement between the registry (JPRS) and registrar (designated operator), which is subject to differ by registrar. For example, a particular registrar indicated it will not approve the transfer when requested confirmation by JPRS if the domain name registrant does not request transferring out in advance.
However, as Table 1 demonstrates, an incident of domain hijackings occurred using this method of fraudulent transfer. The following approaches, including the strengthening of management systems and use of services provided by registrars, are recommended for domain name registrants to protect their domains. These measures will mitigate the risk of approving domain transfers by error at the least.

- Domain name administrators shall always be reachable. Having multiple domain name administrators assigned will reduce risks of miscommunication during reassignments and change of contact information, as well as approving domain transfers by error.
- Check your registrar's domain transfer procedures in advance. If issues are identified, discuss countermeasures.
- Regularly inspect the registration status of the domain name owned by your organization
- Use "domain lock" service that prevents registered information being changed easily

Domain names are an integral part of a company's brand image as well as an essential component in providing IT services. It is recommended for companies to centrally manage their registered domains and use this report as an opportunity to reflect on the company's domain management.

2.2. IoT Devices as an Entry point

IoT is the abbreviation for the "Internet of Things." Compared to how the conventional internet was used to connect computers, IoT networks various objects via the internet such as household appliances including TVs and cameras, thermometer sensors and power meter sensors. The improved performances of IoT devices have been remarkable, highlighted by the launch of smart speakers with virtual assistants offering hands-free activation and compact LinuxKits such as Raspberry Pi that allow consumers to craft IoT devices themselves. As the rising popularity of IoT devices enhance convenience, however, more focus needs to be placed on security because they are always networked. For example, the chipsets used in smart speakers are more sophisticated than smartphones from several years ago [10], and Raspberry Pi is a computer in itself, being potential targets for malicious use. For attackers, IoT devices are already targets worth preying on. The malware "Mirai" that was first found in 2016 and used in a widespread DDoS attack on IoT devices with weak security configurations [11] continues to be a significant threat as of the first quarter of FY2019, with new variants identified [12].

Previous IoT device incidents targeted the devices themselves, such as breaching information inside [13] and incorporating them to botnets that land DDoS attacks. However, during the first quarter of FY2019, an incident in which IoT devices became entries to invade an internal network and steal confidential files was reported.

According to a report issued by NASA on June 18, 2019, a hacker infiltrated its network in April 2018 and stole confidential data from the Jet Propulsion Laboratory (JPL), including data related to the Mars Curiosity Rover mission (500 MB of data from 23 files) [14]. The perpetuator was reportedly able to gain access to the network by targeting an unauthorized Raspberry Pi that was attached to the JPL network (See Figure 3). The hack went undetected for about 10 months, and the data was then stolen by exploiting vulnerabilities in the network.

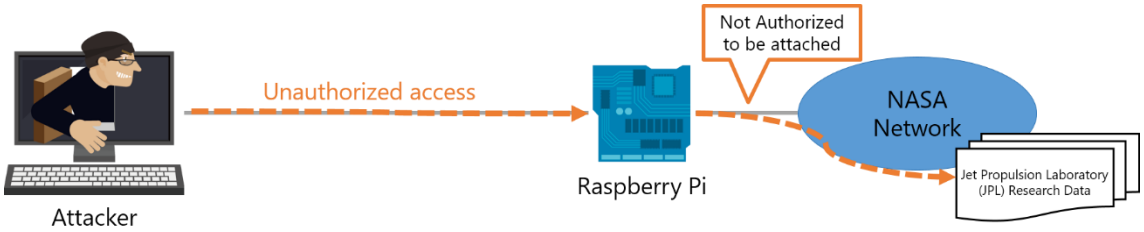


Figure 3: Illustration of how the network was invaded
(Prepared by NTTDATA-CERT)

The Raspberry Pi that was used as an entry should only have been attached to the internal network after registering on the security database (ITSDB) and undergoing security reviews and obtaining approval by the Office of the Chief Information Officer (OCIO) in advance. However, it was reported that this security database was often not updated due to malfunctioning, which led to delays in registering the device, consequently leaving the compromised Raspberry Pi not logged (See Figure 4). The JPL therefore couldn't identify and manage the devices that were connected to the network. The report also indicated additional issues, including the fact that the system's vulnerabilities were left unfixed for 6 months and the JPL's failure to appropriately segment its internal network.

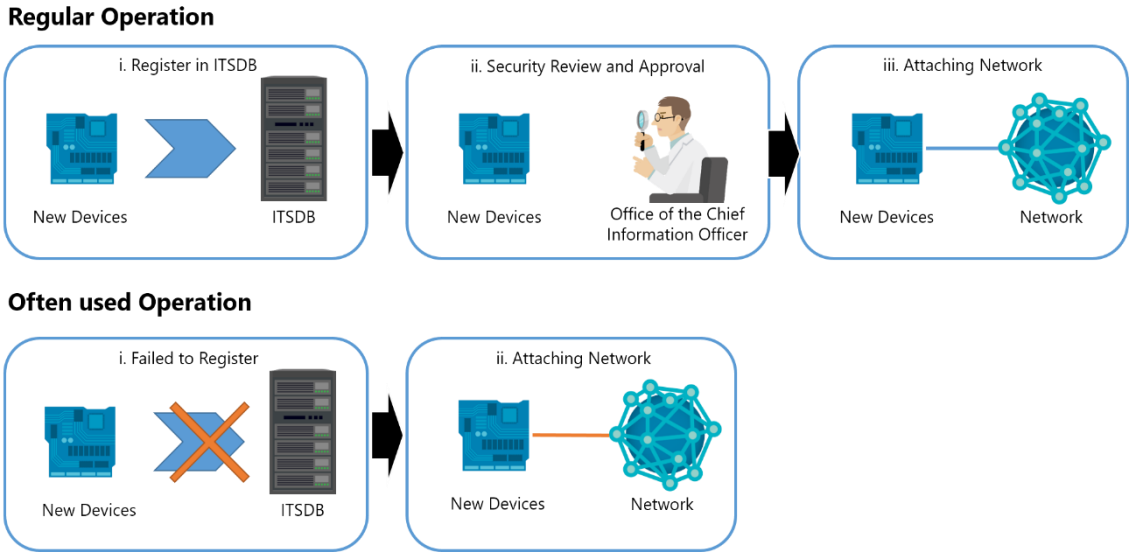


Figure 4: Device management operation by NASA
(Prepared by NTTDATA-CERT)

Although NASA reports this incident as a targeted attack, the issues pointed out in its report may be relatable to other organizations.

The first issue was the devices connected to the internal network weren't databased properly. Like the NASA case, if devices connected to the network that became entry points aren't properly logged, the identification of unauthorized intrusions and their causes may lag behind. Given IoT devices are now also potential targets, they should be managed in the same way PCs and servers are.

The second issue was that security-related protocols weren't followed. The first issue wouldn't have occurred if the protocols were followed. For NASA, the protocols became challenging to follow after security database malfunctions, leading to procedures being skipped at its staff's discretion. This problem has also been addressed during the keynote at the 2016 CODE

BLUE security conference, which stated “Restrictive protections are easily and often circumvented, [15]” and added this frequently causes significant incidents to occur. Therefore, it is recommended to implement security measures that won’t cause inconvenience to users and don’t depend on the users’ manual operations yet ensures safety. For NASA’s case, a framework that won’t involve users’ manual operations, such as having the Raspberry Pi automatically connect to an isolated network temporarily when it first accesses the network to be logged in the security database, is desirable.

3. Data Breach

There were many data breach incidents reported during the first quarter of FY2019 as well. In Japan, multiple companies reported data breaches following unauthorized access. Among them, some reported being victims of password list attacks, which indicate that information leaked through large-scale data breach incidents such as from "Collection #1" may be exploited, as predicted in our report in the fourth quarter of FY2018 [16]. An attacker called "Gnosticplayers" who sold massive volumes of personal information over the dark web 4 times in total during the fourth quarter of FY2018 has disclosed 65.5 million pieces of information in April with the intention of selling them [17].

As forecasted in our report in the fourth quarter of FY2018, there have been increasingly more cases of web skimming reported, as well as data breach incidents due to defective configurations in the database system. The following are summaries of these cases.

3.1. Continued cases of web skimming

There have been multiple reports of damage believed to be caused by web skimming. This class of attack has been on the rise since 2018, with its methods becoming more advanced. During the first quarter of FY2019, additional EC website development platforms other than Magento were confirmed as being targeted, in addition to new attacker groups being reported. The skimming tactics used for Magento, having been preyed on multiple times to date, have improved [18]. Attackers are now targeting and attacking EC website development platforms. Companies that run EC sites need to up their security measures.

Security company TrendMicro reported on a new cybercrime group called "Mirrorthief" that runs skimming attacks [19]. Mirrorthief attacked online stores run by universities, causing 201 universities in the US and Canada to fall victim. These universities used PrismWeb, an EC site development platform designed for universities and developed by PrismRBS. Mirrorthief injected JavaScript libraries used on PrismWeb with a skimmer script in its attacks. As proven in this incident, multiple online stores will be compromised at once and lead to significant damage when attackers target EC site development platforms and libraries.

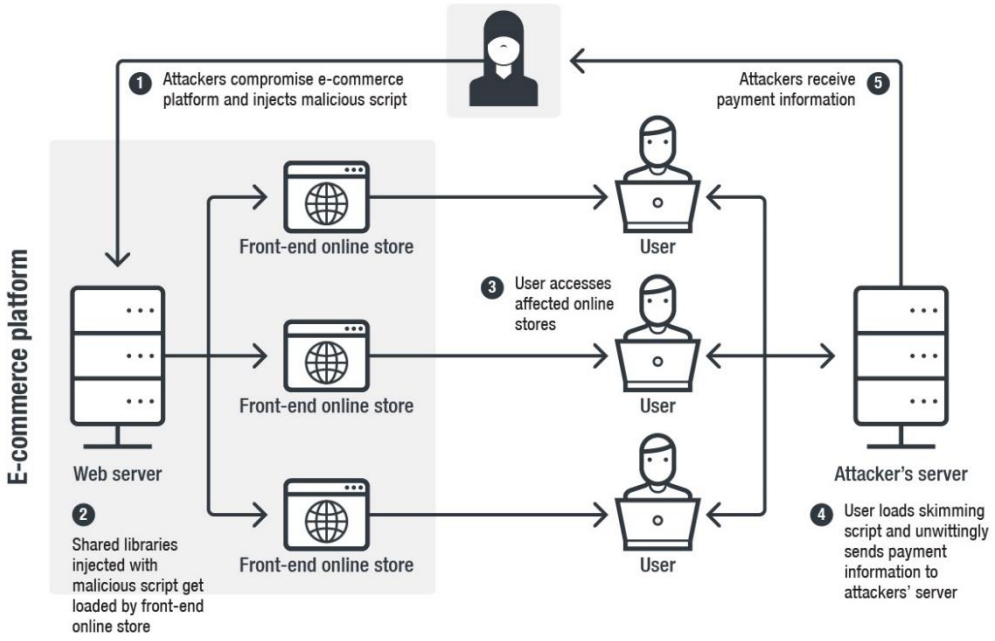


Figure 5: Newly identified web skimming scheme
(Reprinted from Trend Micro's Security Intelligence Blog [19])

More e-commerce website development platforms targets have been confirmed. Online security company RiskIQ reported on its website on May 1 that platforms other than Magento such as OpenCart and OSCommers are being targeted [20]. Our report in the fourth quarter of FY2018 predicted that there will be more widespread damage in the event major EC website development platforms in Japan are targeted. On May 9, EC Cube posted an alert on its website, warning, "IMPORTANT: Credit card data skimming incidents through website manipulations are increasing." [21]. The company's EC site development platform EC-CUBE is the most popular platform in Japan used to construct online stores. According to the warning, the platform's Version 2 series is particularly vulnerable, with multiple incidents already reported. Companies that run online stores using EC-CUBE need to check their versions and security measures implemented.

EC Cube's alert [21] notes that users with inadequate security measures are vulnerable to attacks, and provides a checklist and suggested countermeasures. The following is a translation of the specific checklist and countermeasures posted in Japanese by EC Cube in its alert.

Table 2: Checklist items and countermeasures by EC CUBE
(Reprinted from the EC-CUBE website [21])

1. **Check for manipulations**
   If you find signs of alterations such as examples described below, immediately close your website temporarily and consult someone who has technical knowledge.
   - JavaScript codes you don't recognize appear on the purchase confirmation screen, etc.
   - A fraudulent URL on the credit card entry screen that appears during purchasing

2. **Is the administrative URL "/admin/" or something easily guessable?**
   If your URL for the administrative screen hasn't been changed and is still "/admin/", please change this as soon as you can because you are providing easy access to attackers. For EC-CUBE2.11 or later versions, the administrative screen URL may be changed during installation or from the administrative screen after installation.
   See "2. How to change the administrative screen URL" on our Manual to Change Settings for instructions on how to change the URL.

3. **Are access restrictions enabled for the administrative screen?**
   If the login screen for administrative controls is easily accessible externally, the administrative screen may be logged in during password brute-force attack or other cybercrime.
   In particular, if the administrative screen URL is "/admin/" and easily accessible, your website is vulnerable to attacks. Please enforce security measures as soon as you can so that unauthorized persons won't be able to access the screen.
   - Set IP restrictions (prohibit access from external parties)
   - Enable basic authentication (set a password for the administrative screen)

   See "3. Setting access restrictions for the administrative screen" on our Manual to Change Settings for instructions on enabling access restrictions.

4. **Check to see whether directories on EC-CUBE that shouldn't be public are public**
   If EC-CUBE directories such as "/data" and "/install" are made public on the operational environment, data including access information to the administrative screen, backup files and uploaded CSV files may be breached.
   Delete /install after completing installation and enable access restrictions to the /data directory.
   Reference (in Japanese)) https://nob-log.info/2013/05/25/wrong-installation-eccube-is-dangerous/ See "4. How to deny access to the data directory" on our Manual to Change Settings for instructions on doing this.

5. **Is security guaranteed on your server, CMS, etc.?**
   Check with your server administrator to see whether vulnerabilities in your server OS and middleware have been fixed.
   If you have CMS such as WordPress or Drupal, or applications that connect to other file operations and databases, also check if vulnerabilities in each of these applications and plugins have been fixed as well.

As mentioned in “1” in Table 2, you should regularly check for unconfirmed JavaScript or other signs of manipulations, in addition to implementing security measures to guard from attacks. It is also important to ground fundamental security measures on surrounding environments, including EC website development platforms, to avoid these attacks. ”5” in Table 2 mentions that OS, database and CMS vulnerabilities may be exploited and escalate to EC sites being compromised. In fact, there are multiple intrusion routes for attackers to breach e-commerce websites. Security measures are necessary for all environments used, and not just for the platform that builds EC sites.

3.2. Data breach due to inadequate database configurations

During the first quarter of FY2019, there were many data breach incidents reported due to inadequate database configurations. In addition to making sensitive information in the inadequately configured database, there were attacks reported in which the attacker hacked into the database, compromised and then deleted the confidential information to demand ransom in exchange for restoring the data.

According to a May 17 article published by computer help site Bleeping Computer, 12,000 pieces of data were deleted on the online MongoDB in a span of only 3 weeks [22]。Only a ransom note demanding money in exchange for their data and the perpetuator's contact information were left behind in the database.

In addition, GitHub and GitLab also experienced multiple incidents between April and May in which data were deleted after unauthorized access and demanded money [23]. GitHub and GitLab are cloud-based repository systems that centrally manage data including source codes for software development and maintenance. In light of these incidents, make sure access restrictions are appropriately configured for database systems and cloud-based repository systems, as well as enforce strict security measures such as correctly managing authentication information.

Table 3 below lists attacks reported in the first quarter of FY2019 caused by inadequate configurations.

Table 3: Incidents caused by inadequate DB configurations

Date	Overview	Damage
4/16	India's major search engine JustDial's database was reported to be exposed and had personal information publicly available since 2015 [24].	100 million users
4/18	A MongoDB named "doroshke-invoice-production" was discovered to be publicly available [25]. The database contained sensitive information on drivers registered on Iran's taxi-hailing app Tap30.	6.7 million records
4/18	Eight databases containing LinkedIn user information were found open and unsecured [26]. The total size of all the databases was 229 GB.	60 million records
4/29	An open and unprotected database impacting up to 65% of US households was discovered [27]. This data breach is very dangerous, given the extensive scale and the nature of the data that directly links to personal information.	80 million households

Date	Overview	Damage
5/9	A SMS bomber had a MongoDB instance open and unsecured [28]. User information speculated to be targets were left accessible to the public.	80 million records
5/13	An unsecured MongoDB instance belonging to website MedicareSupplement.com run by TZ Insurance Solutions was discovered [29]. The data cache contained personal information and health details.	5 million records
5/14	An unprotected ElasticSearch database was discovered, which contained personally identifiable information belonging to nearly 90% of Panama citizens [30].	3.4 million records
5/16	An unsecured ElastiSearch database was discovered, which contained personal information of individuals who participated in requests for free product samples, sweepstakes and surveys in the US [31].	8 million people
5/20	A database containing account information of Instagram users was found online and unsecured [32]. This contained account information of celebrities and brands.	49 million records
5/24	Records including bank account information, Social Security numbers, driver license images and tax records were accessible to the public on the website of First American Financial, a company that offers services such as title insurances. [33]	885 million files

4. Vulnerabilities

Hosts of vulnerabilities were reported during the first quarter of 2019; a total of 5,207 cases were reported, which is 437 more than those reported during the fourth quarter of FY2018 [34]. The vulnerabilities reported on the Oracle WebLogic Server and Windows Remote Desktop Services particularly garnered attention.

4.1. Oracle WebLogic Server vulnerabilities

News on the Oracle WebLogic Server's vulnerabilities made many headlines during the first quarter of FY2019. On April 16, Oracle released its quarterly Critical Patch Update [35]. The following day, on April 17, a vulnerability of the Oracle WebLogic Server not covered by the Critical Patch Update was published on the China National Vulnerability Database (CNVD) as CNVD-C-2019-48814 [36] and became known as a zero-day vulnerability. PoC codes were published for this vulnerability (CNVD-C-2019-48814) on April 25. And on April 26, Oracle officially announced this vulnerability (CVE-2019-2725) and released a patch to fix this in its out-of-band security alert [37].

On June 15, Chinese security company KnownSec 404 Team reported an additional Oracle WebLogic Server vulnerability [38]. Oracle addressed this vulnerability (CVE-2019-2729) on June 18 in an irregular release [39]. Although this vulnerability (CVE-2019-2729) was initially announced as stemming from CVE-2019-2725, Oracle corrected this in a blog article dated June 18 that they two vulnerabilities are different.

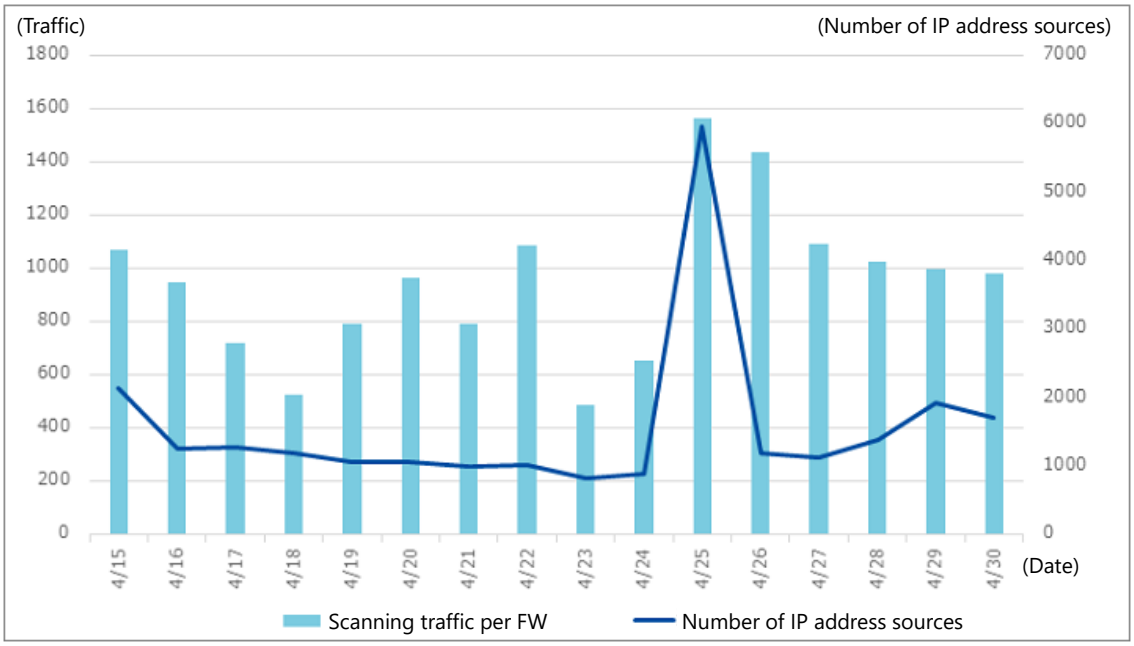


Figure 6: Number of scans for 7001/tcp and number of source IP addresses (Reprinted from wizSafe Security Signal [40])

According to an investigative report by Internet Initiative (IIJ) [40], the PoC codes for the Oracle WebLogic Server vulnerability (CVE-2019-2725) published on April 25 instigated attacker activities. According to Figure 6, the number of port scans targeting 7001/tcp increased on April 25 compared to normal levels, with the number of source IP addresses logged jumping to 9 times more. On the following day on April 26, a cryptocurrency miner was uploaded on Oracle WebLogic Server and attackers lured users to this URL to have them downloaded.

Figure 7: PoC code request and response

(Reprinted from the NTT Data Intellilink Corporation website [41])

A detailed walkthrough of the method used for the attacks is available on an article by NTT Data Intellilink (in Japanese) [41]. To exploit the vulnerability (CVE-2019-2725), a malicious HTTP POST request was sent to the port (TCP 7001) used for the Oracle Weblogic Server's administration console to execute arbitrary OS commands. Figure 7 shows the malicious request sent to the targeted server and its response. The area highlighted in blue is the OS command in which the attacker executes "cat/etc/passwd" and have its results saved on a file named "favicon.ico" under the directory used by the wls9_async component on Oracle WebLogic. This OS command is executed with the same privilege as the Oracle WebLogic Server process.

4.2. Remote Desktop Services vulnerabilities

On May 14, Microsoft released security updates for a vulnerability (CVE-2019-0708) in its Remote Desktop Services [42]. If this critical security called BlueKeep is exploited, attackers can remotely execute arbitrary codes with no authentication by sending malicious codes via the data path for Remote Desktop connections. In addition, Microsoft stated in its blog article that "the vulnerability is 'wormable', meaning that any future malware that exploits this vulnerability could propagate from vulnerable computer to vulnerable computer in a similar way as the WannaCry malware spread across the globe in 2017 [43]. The level of severity can be backed through Microsoft's release of emergency security update programs for end-of-life systems including Windows XP and Windows 2003 Server [44]. The series of alerts issued by various security organizations garnered significant attention to this vulnerability. The events pertaining to this vulnerability are listed in Table 4 below.

Table 4: BlueKeep vulnerability-related events

Date	Company	Overview
5/14	Microsoft	The BlueKeep vulnerability for Remote Desktop Services (CVE-2019-0708) was announced [43], and pointed out it can be exploited to program WannaCry-level malware. The company's unusual step of releasing security updates for out-of-support systems Windows XP and Windows Server 2003 in addition to updates for in-support Windows 7 and Windows Server 2008 R2 and Windows Server 2008 also drew attention.
5/24	Microsoft	Also released a security update for out-of-support Windows Vista systems [44].
5/28	Errata Security	Reported its scanning results that indicate 1 million computers remain vulnerable [45].
5/30	Microsoft	Posted a reminder to patch the vulnerability with its security update [46]. Following Errata Security's report on its scanning results, Microsoft issued an alert on its official blog, emphasizing the vulnerability's level of danger by mentioning the EternalBlue cyberattack exploit used in WannaCry.
6/4	NSA	The US National Security Agency (NSA) issued a warning of the BlueKeep vulnerability [47]. The NSA's very unusual warning issued to the general public became significant news.
6/7	Morphus Labs	A brute-force attack targeting 1.5 million RDP servers by a botnet called GoldBrute was discovered [48]. This attack also gathered attention amid warnings issued by many companies on the BlueKeep vulnerability.
6/17	CISA	The Department of Homeland Security (DHS)'s Cybersecurity and Infrastructure Security Agency (CISA) announced the BlueKeep vulnerability also exists in Windows Vista and Windows 2000 [49]. It reported that it actually confirmed Windows 2000 is vulnerable to BlueKeep.

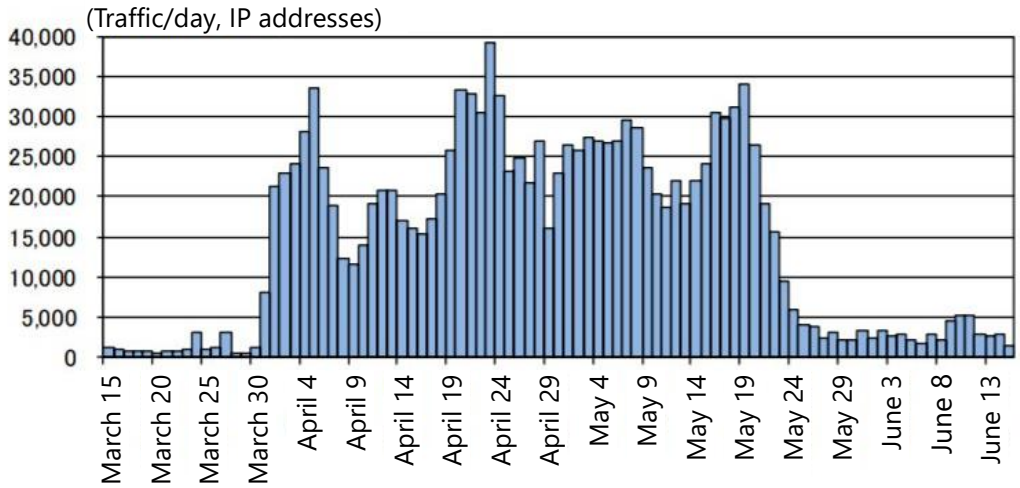


Figure 8: Accesses targeting Remote Desktop Services
(March 15, 2019-June 15, 2019)
(Reprinted from the National Police Agency's @police website) [50])

Figure 8 is a graph that indicates traffic that targeted the BlueKeep vulnerability (CVE-2019-0708) in Remote Desktop Services [50]. According to this, traffic increased from late March through late May.

The BlueKeep vulnerability became a significant topic as it was referred to as being "wormable" and capable of causing WannaCry-level attacks. For the vulnerability exploited by WannaCry, there was a time lapse from when the vulnerability was announced until security update programs were released, with an alert issued much later. On the contrary, the BlueKeep vulnerability and security update program were announced and released at the same time, with numerous alerts issued immediately afterward. There have been no reports of significant damage or malware in connection to BlueKeep at the moment, indicating that the alerts issued by security organizations and companies' responses were successful.

4.3. Other vulnerabilities

The table below lists zero-day vulnerabilities and exploited vulnerabilities reported during the first quarter of FY2019.

Table 5: Zero-day vulnerabilities reported during the first quarter of FY2019

Date	Product	Vulnerability No.	Overview
4/9	Windows	CVE-2019-0803 CVE-2019-0859	Microsoft addressed 2 zero-day vulnerabilities in April in its Monthly Rollup [51] [52]. Both were elevations of privilege vulnerabilities impacting Win32k.
5/10	WhatsApp	CVE-2019-3568	Facebook released a security alert to address a vulnerability in WhatsApp [53]. Devices may be hacked if the vulnerability is exploited.
5/24	Windows Internet Explorer	-	A security researcher at Zscaler reported 2 local privilege escalation vulnerabilities in Windows and 1 sandbox bypass vulnerability in IE [54]. The POCs were also published at the same time.
5/24	macOS	-	Intego disclosed a zero-day vulnerability in macOS Gatekeeper bypass that allows software to be run as 'safe' [55]. Malware were also confirmed.
6/11	SymCrypt	CVE-2019-0865	A Google Project Zero researcher disclosed a zero-day vulnerability within the cryptographic library SymCrypt that can perform a DoS attack on Windows servers [56].
6/24	Firefox	CVE-2019-11707 CVE-2019-11708	Mozilla released a version that patched the zero-day vulnerability that causes crashes from JavaScript processing [57].

Table 6: Vulnerabilities exploited during the first quarter of FY2019

Date	Product	Vulnerability No.	Overview
4/10	WinRAR	CVE-2018-20250	The Office 365 Team picked up a phishing mail campaign that exploited a vulnerability [58].
4/11	Jenkins	CVE-2019-1003000 CVE-2019-1003001 CVE-2019-1003002	Non-profit foundation Matrix.org's server suffered a cyberattack after Jenkins' known vulnerability was exploited. Credentials were stolen, allowing access to the production environment [59].
4/17	ThinkPHP	CVE-2018-20062	Sucuri reported an increase in attacks that upload cryptominers aiming at Versions 5.1x/5.2x of ThinkPHP [60].
4/23 5/10	SharePoint	CVE-2019-0604	The Canadian and Saudi Arabian governments reported series of attacks on SharePoint servers [61] [62]. Although both planted the China Chopper malware, there is no evidence the attacks are connected.
5/7	Confluence Server	CVE-2019-3396	TrendMicro discovered an attack that exploited the vulnerability in the software Confluence reported by Atlassian in March [63].
6/7	Office	CVE-2017-11882	Microsoft warned on Twitter that there is an active malware campaign that carries the known CVE-2017-11882 exploit [64].

The number of vulnerabilities reported has been increasing year after year. The time span from when the vulnerability was published to attack code breaches and actual attacks has shortened. Given the wide-ranging types of attacks, anyone can be victimized by attacks that exploit vulnerabilities.

Companies need to prevent damage caused by attacks targeting their critical systems. To appropriately respond, companies need to correctly evaluate the impact of vulnerabilities and determine whether responses are necessary after first quickly obtaining information about these vulnerabilities. In addition, immediate action needs to be taken to patch these vulnerabilities if they are determined to generate significant impact. It is essential to have frameworks and systems developed and readily available. However, it is virtually impossible to respond to all vulnerabilities given the expansive and ever-increasing number of exploits reported. During FY2018, there were 2,000 disclosed vulnerabilities with CVSS base scores with "High severity" alone. Base CVSS scores are calculated based on the Base Metrics of the Common Vulnerability Scoring System (CVSS) V3. Although the CVSS base score may be used to determine the impact of a vulnerability or to determine whether responses are necessary, they are insufficient in quickly and accurately evaluating and making decisions on the massive number of vulnerabilities existing. Configurations, network structures and additional security measures needed differ by system. For example, even if the CVSS base score determines a vulnerability as "High severity," some companies and systems may not be affected when attackers attempt to exploit the vulnerability.

Rather than processing all information pertaining to vulnerabilities, it is recommended that frameworks and systems tailored to the organization are developed, such as devising an efficient method to select vulnerabilities that significantly impact the organization's system, or focusing resources on important systems to quickly respond.

5. Malware/Ransomware

5.1. Emotet, the malware that continues to evolve

Emotet, first identified in 2014, continues to evolve and acts as a significant threat even after 5 years. It was initially discovered as a banking Trojan that steals online banking IDs and passwords. And around 2015, Emotet grew into a multi-purpose malware with diversified functions and packed with multiple modules. After self-extending functions were added around 2017, some versions that hijack massive amounts of emails from victims were identified in 2018. Currently, Emotet infects users through spam campaigns and has caused considerable damage as an information theft malware and ransomware.

According to security company Proofpoint's report [65], 61% of malicious payloads delivered by emails between January and March 2019 were botnets, of which most were attributable to Emotet. Proofpoint's Chris Dawson points out that Emotet is module-based and highly flexible, structures a sufficiently large botnet and is adept at distributing campaigns in a wide range of geographies and languages to increase its global footprint.

On April 11, news media ZDNet reported on the tactics of Emotet infections that use old email conversation threads [66]. This tactic is characteristic in that emails with malicious URL links and files attached that appear to be replies from actual people or organizations are sent to the targets. This makes recipients more prone to being convinced they are real replies and open the URL links or files attached, given actual email threads are used. This is a very advanced tactic that is closer to being a targeted attack rather than a randomized attack. As of date, email threads collected from machines infected earlier than November 2018 are being exploited. If emails continue to be collected from compromised machines, it can be predicted that the attackers will continue with this tactic by exploiting the newly acquired emails.

On April 25, security company TrendMicro reported on a new Emotet sample identified in late March 2019 [67]. The new samples demonstrate different post-infection traffic with C&C servers. Out of the many changes Emotet has gone through over the years, this was the first time a different traffic technique was confirmed. Previously, Emotet did not use an URI path. However, because increasingly more security products raise red flags for empty URI paths, the new Emotet samples inject random words to avoid detection. In addition, Emotet previously encrypted data into the Cookie header when using an HTTP GET request. The new Emotet samples, however, changed to the HTTP request method to POST and injects the data

into the body of the HTTP message. This change adds another layer of complexity to help the malware evade detection or delay further investigation if it is detected.

Emotet continues to be a significant threat, even after 5 years since its first appearance, by incorporating self-expanding functions and methods to evade detection. Its example proves that cyberattack tactics are evolving and being fine-tuned on a daily basis. With that said, security measures also need to adapt to attack tactics and should be ongoing. Multifaceted approaches that address malicious email and detection of malicious communications, for example, need to be effective at the same time in order to catch up to attacks like Emotet that constantly and flexibly evolve. TrendMicro's article stresses the need to implement multilayered and proactive approaches that will protect the gateway, endpoints, networks and servers to combat threats like Emotet [67].

5.2. Other reported incidents

The first quarter of FY2019 continued to see various companies and organizations affected by malware and ransomware attacks. In particular, many cities in the US have reported being struck by ransomware attacks. Reported incidents and damage caused by malware and ransomware during the quarter are listed in Table 7 below.

Table 7: Other reported malware and ransomware attacks and damages

Date	Organization	Overview
3/30	Albany, New York	Albany was affected by a ransomware attack [68]. Although some data were lost, they were reportedly restorable.
4/2	Genesee County, Michigan	The county was affected by a ransomware attack [69]. Although goals were initially set to restoring operations by 4/8, news reported that the country continued to be affected as of 4/17.
4/4*	Bayer	German pharmaceuticals company Bayer announced it was affected by a malware called WINNTI last year [70]. Its statement claims there is no evidence of data breach.
4/9	Kanagawa University	The university's email management system was affected by ransomware [71]. The server contained sensitive information including student names, email addresses and default passwords.
4/13	Stuart, Florida	The city was infected by ransomware Ryuk through a phishing email [72]. The server was forced to shut down.
4/22	Amarillo, Texas	The entire network was shut down following a ransomware attack [73]. Work for more than 550 employees was disrupted.
4/25	Aebi Schmidt	The company's email systems and several other systems were disrupted following a ransomware attack [74]. It prevented further infections by temporarily switching off the systems.
5/7	Baltimore City Hall, Maryland	The Baltimore government was attacked with ransomware RobbinHood. Many of its computers became locked, leading some services to completely shut down [75].
5/28	Sasebo Kyosai Hospital	The hospital announced it has detected a computer virus from a computed connected to its radiographic inspection equipment [76]. To prevent further infection, the hospital shut down its network.
5/29*	Checkers Drive-In Restaurants	Malware was found in POS systems of 102 of the restaurant's 900 locations in the US [77]. The compromised data included credit card information.
5/29	Riviera Beach, Florida	The ransomware locked files and shut down all the city's services [78]. The city paid $600,000 to recover data.
6/7	ASCO	Aircraft parts manufacturer ASCO was hit by a ransomware attack [79]. Although there were no information breaches, about 1,000 employees were affected due to the disruption in the company's operations.
6/10	Lake City, Florida	Despite disconnecting impacted systems, almost all the city's systems were infected by ransomware [80]. The city paid 42 bitcoins (worth about $500,000).

*Date of announcement, as opposed to when the attack took place

6. Trends by Category

6.1. Trends of government/public sector-led security measures

During the first quarter of FY2019, IoT-related security measures and initiatives were implemented by governments.

Table 8: List of events related to government/public sector-led security measures

No.	Date	Country/Region	Overview
1	April 1	Japan	The National Center of Incident Readiness and Strategy for Cybersecurity (NISC) announced the formation of the Cybersecurity Council based on the Act Partially Amending the Basic Act on Cybersecurity. The Council will primarily work with diverse public and private organizations to share and analyze information on threats, together with devising and sharing countermeasures [81].
2	April 22	Japan	The Ministry of Internal Affairs and Communications announced its First Edition of Guidelines Pertaining to the Standards and Certification of Terminal Devices based on the Telecommunications Business Act [82]. The Guideline prescribes technical standard conformity certification pertaining to security standards for IoT devices and technical standard conformity certification pertaining to terminal devices that use radio waves.
3	April 23	The Netherlands	The National Cyber Security Centrum (NCSC) announced its updating of IT security guidelines for TLS [83]. The guideline prescribes secure TLS configurations. The update added recommending configurations for TLS1.3.
4	April 29	USA	The Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS) issued Binding Operational Directive 19-02 that requires federal government institutions to ensure scanning access to scan vulnerabilities for systems accessible by the internet and remediate vulnerabilities detected within prescribed periods [84].
5	April 29	Japan	News media Kyodo News reported the Japanese government has decided to have the Ministry of Defense develop and possess malware to retaliate against cyberattacks that threaten national security [85].

No.	Date	Country/Region	Overview
6	May 1	UK	News media BBC reported on a proposed legislation that would introduce a labeling system that tells consumers how secure and safe an IoT product is [86]. To obtain this label and market the product, IoT devices would need to have unique passwords by default, clearly state how long security updates would be available and provide a point of contact with information on vulnerabilities available.
7	May 2	USA	President Trump issued an Executive Order on the American cybersecurity workforce [87]. It includes strengthening the federal cybersecurity workforce and hiring of personnel to conduct cybersecurity training.
8	May 14	Japan	News media Jiji Press reported that the Liberal Democratic Party submitted a proposal to PM Abe on responding to cyberattacks [88]. The proposal recommended requiring countermeasures to be devised by critical infrastructure operators and an establishment of the Cybersecurity Agency.
9	May 20	Japan	The Information-technology Protection Agency (IPA) announced a Checklist of Information Security Requirements for Entrance and Exit Management Systems [89]. The Checklist includes security requirements that safeguard anticipated threats in entrance and exit management systems.
10	May 29	Japan	The Council of Anti-Phishing Japan's Technology and System Review Working Group revised anti-phishing guidelines for both operators and users, and published them as 2019 versions [90]. The updated guideline includes trends in 2018 and contents that take into account new anti-phishing technologies.
11	June 11	USA	The National Institute of Standards and Technology (NIST) announced a draft of a white paper on Secure Software Development Framework (SSDF) [91]. It believes following this framework will help mitigate risks associated with vulnerabilities.
12	June 14	Japan	The Ministry of Internal Affairs and Communications announced it will alert users using malware-infected IoT devices [92]. Together with its ongoing NOTICE initiatives, it will issue alerts to users of detected devices through the NICTER Project run by the National Institute of Information and Communications Technology (NICT).
13	June 25	USA	The NIST published a guideline on cybersecurity and privacy risks for when managing IoT [93]. The guideline includes 3 high-level considerations and ways to mitigate the risks.

6.2. Trends on privacy

During the first quarter of FY2019, discussions took place on the utilization of personal data in Japan while many bills were passed by state legislatures in the US on enforcing the protection of such information.

Table 9: List of events pertaining to privacy

No.	Date	Country/Region	Overview
1	April 9	USA	Senator Mark Warner and a group of senators introduced the Deceptive Experiences To Online Users Reduction (DETOUR) Act that will prohibit platforms from using deceptive UI as methods to trick users into handing over their personal data [94]. This bill will apply to large internet platforms with over 100 million active users per month.
2	April 25	Washington, USA	The Washington legislature passed a bill pertaining to the state's data breach notification requirements [95]. The new law, HB1071, requires data breach organizations to notify users if the security incident exposes the users' names in combination with public ID.
3	April 25	UK	News media ZDNet reported the National Cyber Security Center (NCSC) and Information Commissioner Office (ICO) have clarified their roles in the event of data breach incidents [96]. While the NCSC will provide assistance to victim organizations to prevent future attacks, the ICO will monitor and enforce GDPR. The two organizations share anonymized and aggregated information with one another.
4	May 3	UK	HM Revenue and Customs (HMRC) reported that it has notified the ICO it will be deleting the voice files of 5 million taxpayers, gathered without consent and pointed out by the ICO as violating GDPR rules, by June 5 [97]. This issue came into light after complaints voiced by the UK's privacy campaigner Big Brother Watch [98].
5	May 22	Japan	News media Nikkei xTECH reported the government's expert panel compiled a proposal encouraging the government to utilize personal data and link data between public and private organizations [99]. The panel suggested that service structures and data formats should be standardized through running trial experiments in order to have the information bank and data transaction market be more widely used.
6	May 22	Ireland	Ireland's Data Protection Commission (DPC) opened an investigation into Google Ireland [100]. This investigation will probe whether Google's processing of personal data in each of the advertising transaction phases violates GDPR-related provisions.
7	May 30	Maine, USA	The Maine legislature passed an online privacy protection bill [101], which prohibits ISPs from disclosing or selling personal information to third parties without their users' consent.

No.	Date	Country/Region	Overview
8	June 17	New York, USA	The New York legislature passed the Stop Hacks and Improve Electronic Data Security, or SHIELD Act [102]. This bill requires companies to notify to affected individuals within a normal span of 30 days in the event of a data breach. This applies to companies that possess private information of a New York resident, in addition to companies conducting business in the state.

7. Outlook

Like during the first quarter of FY2019, cyberattacks that directly impact money are predicted to continue increasing in the second quarter of FY2019. As opportunities to exchange money online have increased, a lot of credit card information and cryptocurrency information are stored on internet-connected servers and clouds in cyber space. Attackers are preying on data that directly link to money and financial services across the globe to efficiently steal money. Demands for money through ransomware attacks may also continue to be reported.

Attacks targeting credit card information

Reports from the fourth quarter of FY2018 and first quarter of FY2019 both discussed web skimming. Web skimming incidents are continuing to increase as a method to steal credit card information that directly leads to monetization. Users need to check if their services used aren't experiencing data breaches and whether they aren't being charged for purchases they don't recall. Organizations that run EC sites need to re-acknowledge the risks associated with handling user credit card information, check for falsifications and implement security measures, including for surrounding environments. In addition to EC sites, e-money and other services that require registration of credit card information and are gaining popularity may become targets for cyberattacks.

Attacks to Cryptocurrency

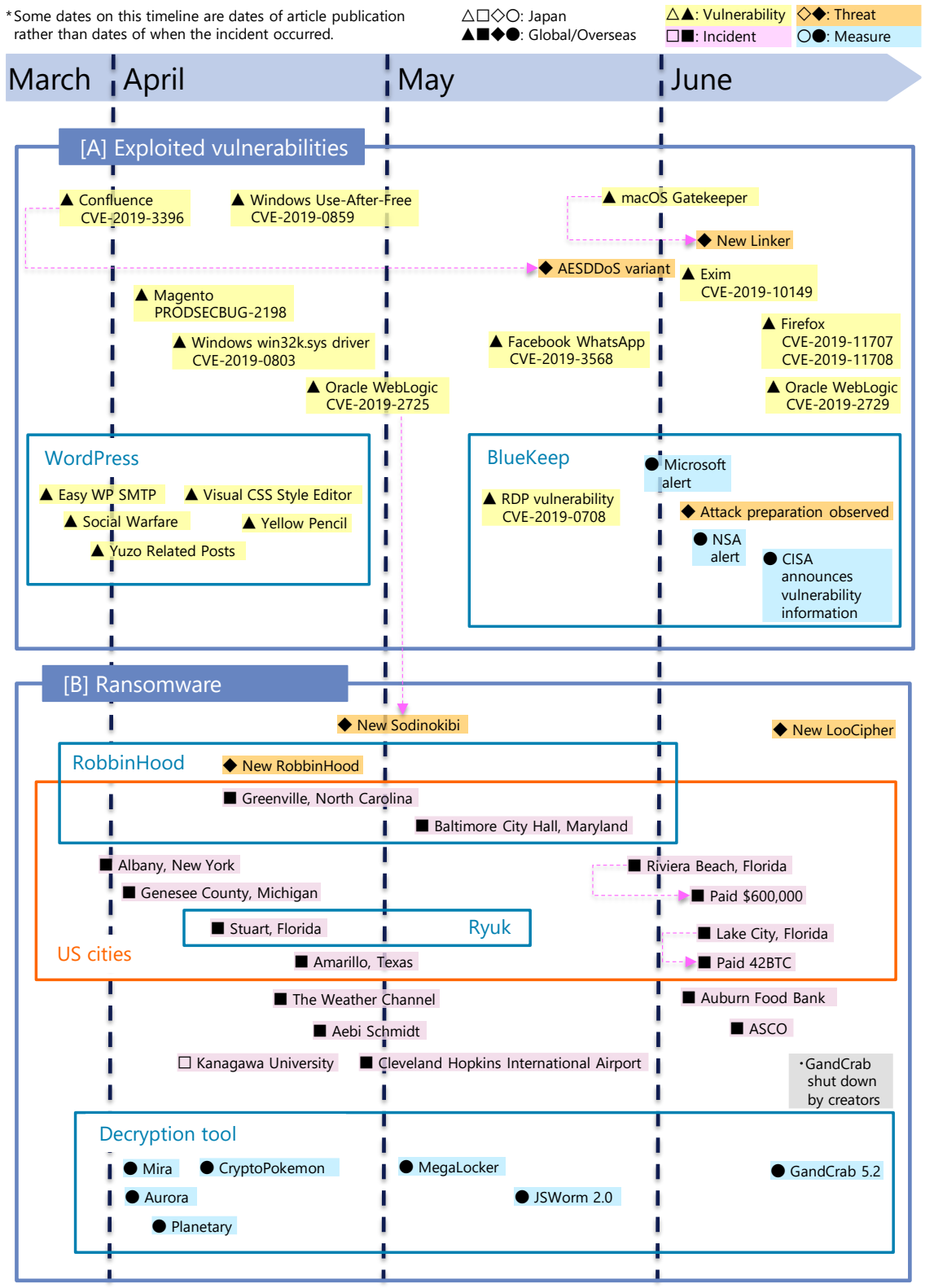
Cryptocurrency is also a great target for cyber attackers to gain money. Our report for the fourth quarter of FY2018 predicted attacks on cryptocurrencies will occur during the first quarter of FY2019 in light of the rising cryptocurrency market prices. In fact, on May 8, major cryptocurrency exchange Binance announced a cyberattack stole 7,000 bitcoins (worth 4.4 billion yen) [103]. Similar incidents may continue as long as market prices are rallying.

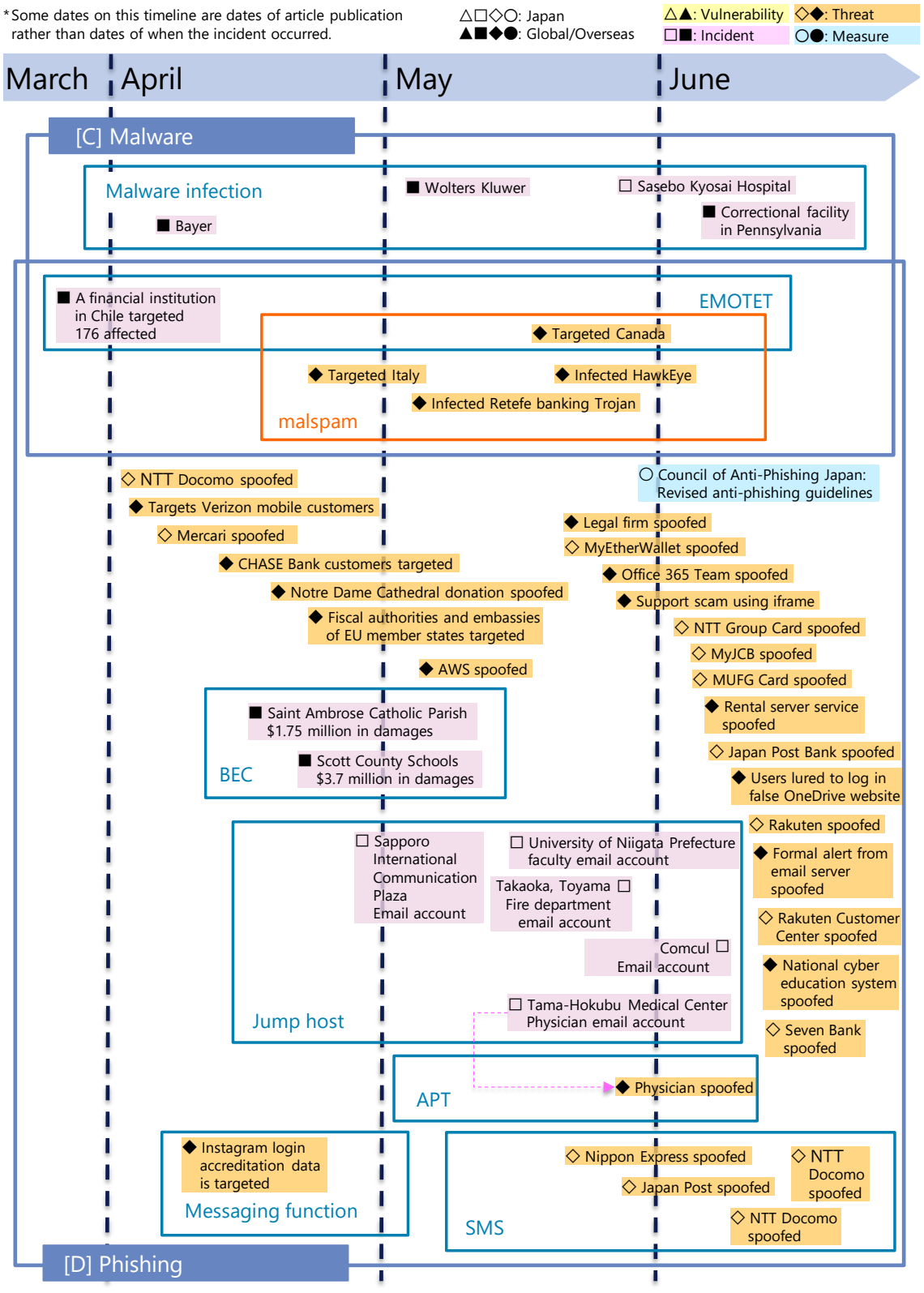
Ransomware attacks targeting local governments

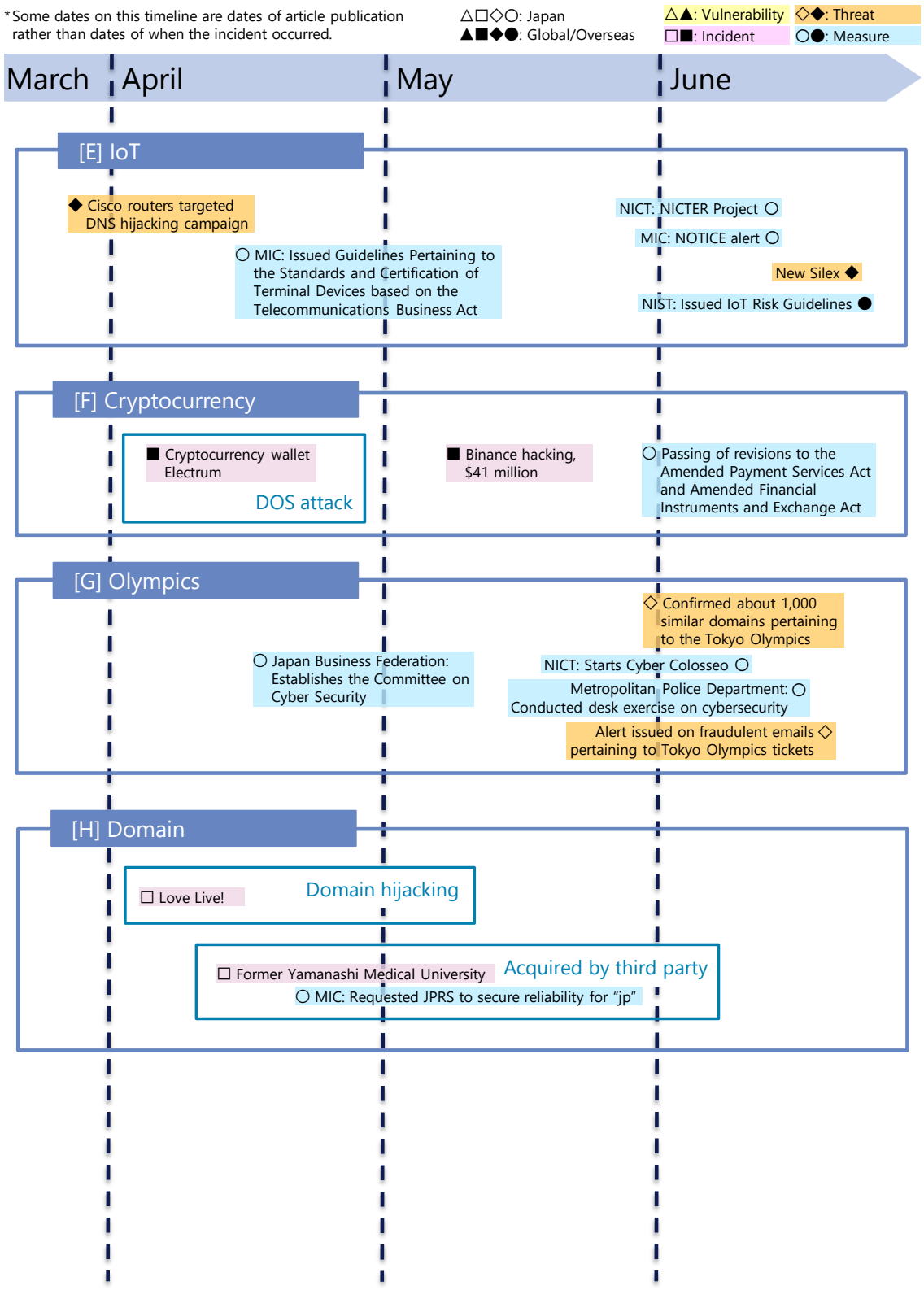
Multiples US cities became victims of ransomware attacks during the first quarter of FY2019. Ransomware attacks that target local government organizations that are not corporate giants or individuals are on the rise. Given local governments are small or medium-sized organizations prone to implement inadequate cybersecurity measures due to lack of budgets and possess systems that impact daily life activities when stopped, they provide excellent environments for attackers. As such, organizations that possess these characteristics may become more popular targets for ransomware attacks. The US Conference of Mayors resolved to not pay ransoms over cyberattacks [104]. It is unclear whether ransomware attackers will

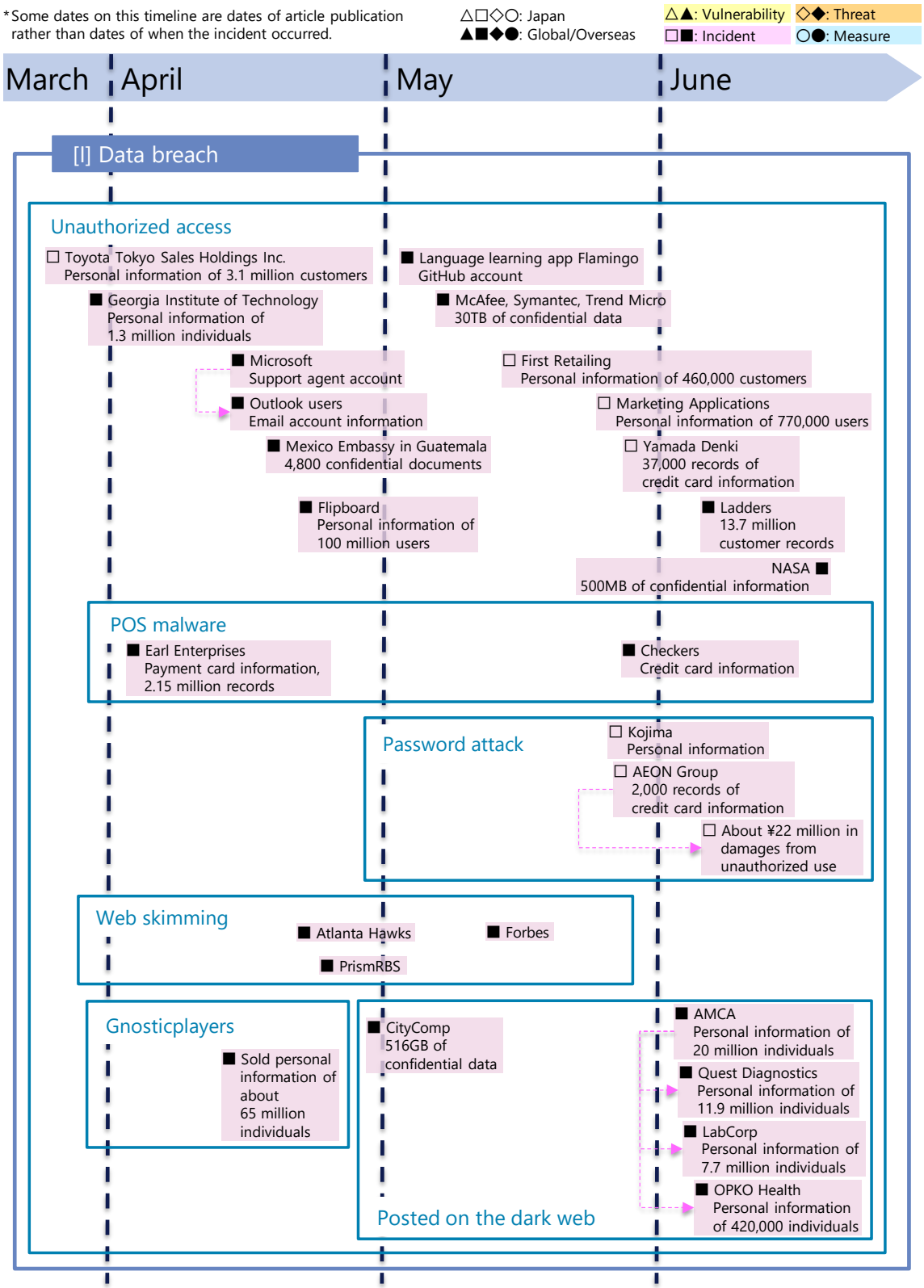
cease targeting city governments in the US. However, this resolution of not paying ransoms simplified cybersecurity countermeasures and incident protocols. Local governments need to consider safeguarding against ransomware attacks, as local governments other than those in the US may become targets. In doing so, they should devise preventative measures for these attacks, as well as decide on how to respond when payment demand is made from a cyberattack.

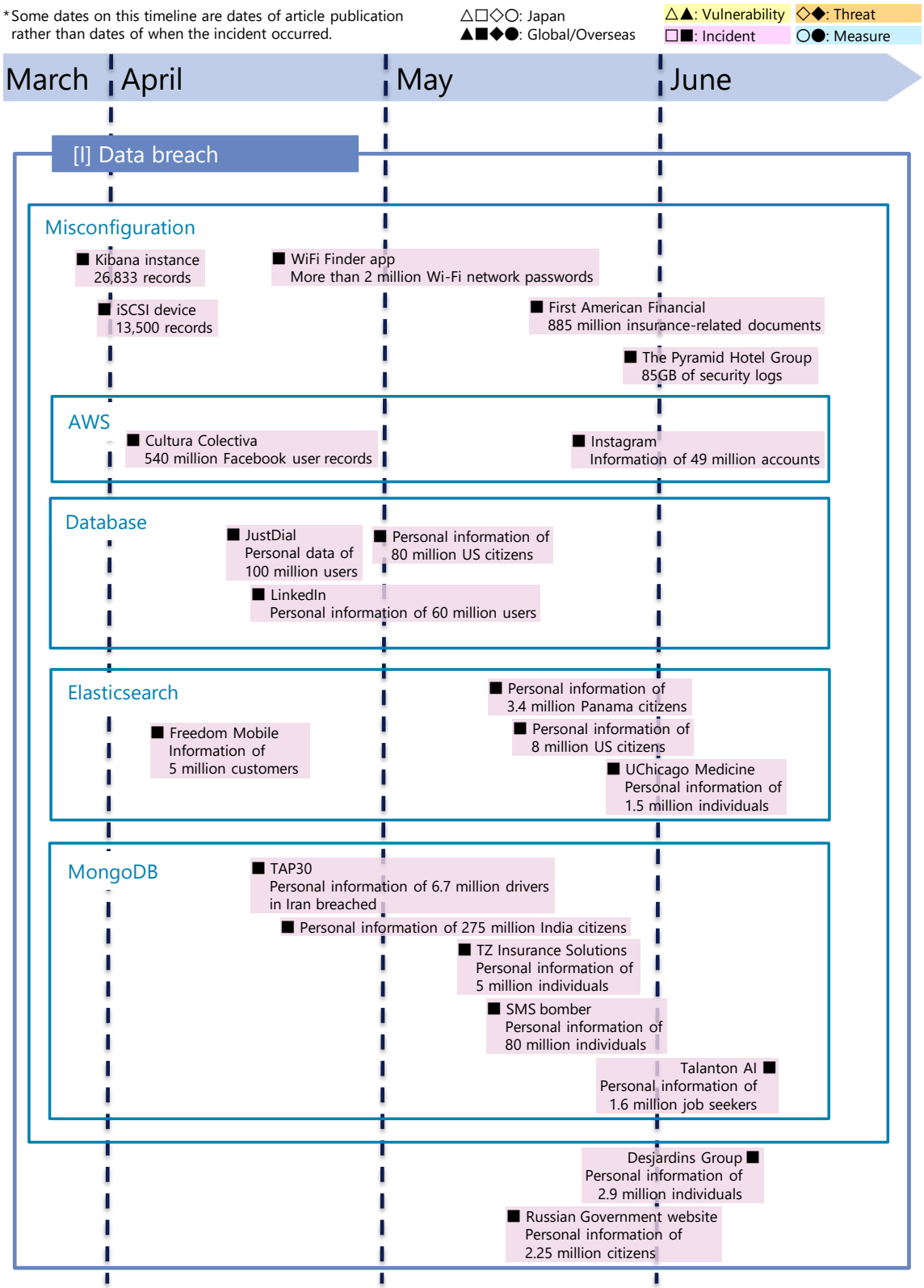
8. Timeline

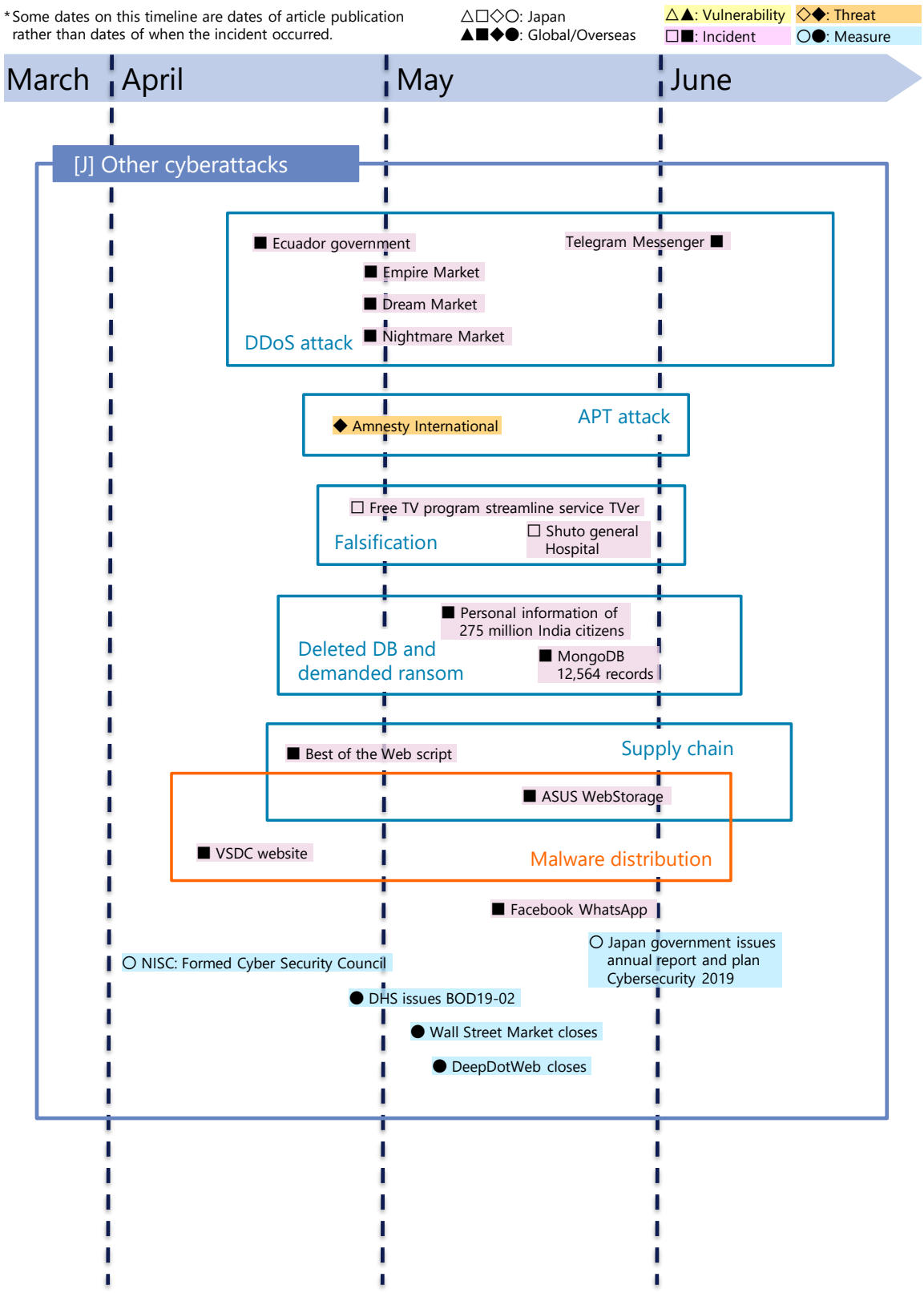












References

[1] サイバーセキュリティ.com編集事務局, “ドメイン名ハイジャックとは？被害事例と対策方法を徹底解説,” CyberSecurity.com, 24 4 2019. [Online]. Available: https://cybersecurity-jp.com/cyber-terrorism/31073.

[2] “アミューズクラフトエロチカ公式Twitterアカウント,” 25 9 2018. [Online]. Available: https://twitter.com/AMUSECRAFT_ero/status/1044539803021135872.

[3] “Internet Archive,” 25 9 2018. [Online]. Available: https://web.archive.org/web/20180925133456/http://amusecraft.jp/. [アクセス日: 5 8 2019].

[4] “シロップ広報担当公式Twitterアカウント,” 15 2 2019. [Online]. Available: https://twitter.com/SYRUP_KOUHOU/status/1096225680004509696.

[5] “Internet Archive,” 29 2 2019. [Online]. Available: https://web.archive.org/web/20190214165224/http://www.syrup-soft.jp:80/mm/index.html.

[6] “タニシ@スク水.jpのTwitterアカウント,” 5 4 2019. [Online]. Available: https://twitter.com/tanishi009/status/1113985953264062464.

[7] “ラブライブ!シリーズ公式Twitterアカウント,” 5 4 2019. [Online]. Available: https://twitter.com/LoveLive_staff/status/1113871689128005634.

[8] “Internet Archive,” 4 4 2019. [Online]. Available: https://web.archive.org/web/20190404173940/http://www.lovelive-anime.jp/.

[9] Japan Registry Services Co., Ltd., “汎用JPドメイン名登録申請等の取次に関する規則,” Japan Registry Services Co., Ltd., 15 6 2016. [Online]. Available: https://jprs.jp/doc/rule/toritsugi-rule-wideusejp.html.

[10] iFixit, “Amazon Echo Dot 2nd Generation Teardown,” iFixit, 26 6 2018. [Online]. Available: https://jp.ifixit.com/Teardown/Amazon+Echo+Dot+2nd+Generation+Teardown/110989.

[11] State of New Jersey, “Mirai,” State of New Jersey, 28 12 2016. [Online]. Available: https://www.cyber.nj.gov/threat-profiles/botnet-variants/mirai-botnet.

[12] N. Ruchna, “New Mirai Variant Adds 8 New Exploits, Targets Additional IoT Devices,” Palo Alto Networks, Inc, 6 6 2019. [Online]. Available: https://unit42.paloaltonetworks.com/new-mirai-variant-adds-8-new-exploits-targets-additional-iot-devices/.

[13] K. VLADIMIR, “覗き見される映像：無防備なIP監視カメラを悪用するサイバー犯罪者のアンダーグラウンド動向,” Trend Micro Incorporated, 28 6 2018. [Online]. Available: https://www.trendmicro.com/jp/iot-security/special/50202.

[14] Office of Inspector General, “CYBERSECURITY MANAGEMENT AND OVERSIGHT AT THE JET PROPULSION LABORATORY,” NationalAeronautics and Space Administration, 18 6 2019. [Online]. Available: https://oig.nasa.gov/docs/IG-19-022.pdf.

[15] K. Nohl , “[CB16] 基調講演： セキュリティはどれくらいが適量? – How much security is too much? – by Karsten Nohl,” 9 11 2016. [Online]. Available: https://www.slideshare.net/codeblue_jp/cb16-nohl-ja.

[16] NTTDATA-CERT, “グローバルセキュリティ動向四半期レポート(2018年度第4四半期),” 30 5 2019. [Online]. Available: https://www.nttdata.com/jp/ja/news/information/2019/053000/.

[17] Security Affairs, “Gnosticplayers round 5 – 65 Million+ fresh accounts from 6 security breaches available for sale,” 15 4 2019. [Online]. Available: https://securityaffairs.co/wordpress/83904/data-breach/gnosticplayers-fifth-round.html.

[18] BleepingComputer, “Hackers Steal Payment Card Data Using Rogue Iframe Phishing,” 21 5 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/hackers-steal-payment-card-data-using-rogue-iframe-phishing/.

[19] TrendMicro, “Mirrorthief Group Uses Magecart Skimming Attack to Hit Hundreds of Campus Online Stores in US and Canada,” 3 5 2019. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/mirrorthief-group-uses-magecart-skimming-attack-to-hit-hundreds-of-campus-online-stores-in-us-and-canada/.

[20] RiskIQ, “Magento Attack: All Payment Platforms are Targets for Magecart Attacks,” 1 5 2019. [Online]. Available: https://www.riskiq.com/blog/labs/magecart-beyond-magento/.

[21] EC-CUBE, “【重要】サイト改ざんによるクレジットカード流出被害が増加しています（2019/05/09）,” 9 5 2019. [Online]. Available: https://www.ec-cube.net/news/detail.php?news_id=330.

[22] Bleeping Computer, “Over 12,000 MongoDB Databases Deleted by Unistellar Attackers,” 17 5 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/over-12-000-mongodb-databases-deleted-by-unistellar-attackers/.

[23] Bleeping Computer, “Attackers Wiping GitHub and GitLab Repos, Leave Ransom Notes,” 3 5 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/attackers-wiping-github-and-gitlab-repos-leave-ransom-notes/.

[24] The Hacker News, “Over 100 Million JustDial Users' Personal Data Found Exposed On the Internet,” 17 4 2019. [Online]. Available: https://thehackernews.com/2019/04/justdial-hacked-data-breach.html.

[25] SECURITY DISCOVERY, “Iranian Ride-Hailing App Database Exposure,” 19 4 2019. [Online]. Available: https://securitydiscovery.com/iranian-ride-hailing-app-database-exposure/.

[26] “Unsecured Databases Leak 60 Million Records of Scraped LinkedIn Data,” 18 4 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/unsecured-databases-leak-60-million-records-of-scraped-linkedin-data/.

[27] Security Affairs, “Report: Unknown Data Breach Exposes 80 Million US Households,” 29 4 2019. [Online]. Available: https://securityaffairs.co/wordpress/84666/data-breach/80-million-us-households-leak.html.

[28] SECURITY DISCOVERY, “Massive SMS Bombing Operation Uncovered In Passwordless Database,” 9 5 2019. [Online]. Available: https://securitydiscovery.com/massive-sms-bombing-operation/.

[29] Bleeping Computer, “Open Marketing Database Exposes 5 Million Personal Records,” 28 6 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/open-marketing-database-exposes-5-million-personal-records/.

[30] Security Affairs, “Unprotected DB exposed PII belonging to nearly 90% of Panama citizens,” 2019. [Online]. Available: https://securityaffairs.co/wordpress/85462/data-breach/panama-citizens-massive-data-leak.html.

[31] Bleeping Computer, “Unsecured Survey Database Exposes Info of 8 Million People,” 16 5 2019. [Online]. Available: https://www.bleepingcomputer.com/news/security/unsecured-survey-database-exposes-info-of-8-million-people/.

[32] Security Affairs, “Data belonging to Instagram influencers and celebrities exposed online,” 20 5 2019. [Online]. Available: https://securityaffairs.co/wordpress/85905/data-breach/instagram-data-leak.html.

[33] Krebs on Security, “First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records,” 24 5 2019. [Online]. Available: https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/.

[34] IPA, “脆弱性対策情報データベースJVN iPediaの登録状況 [2019年第2四半期（4月～6月）],” 24 7 2019. [Online]. Available: https://www.ipa.go.jp/security/vuln/report/JVNiPedia2019q2.html.

[35] Oracle, “Oracle Critical Patch Update Advisory - April 2019,” 16 4 2019. [Online]. Available: https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html.

[36] CHINA NATIONAL VULNERABILITY DATABASE, “关于Oracle WebLogic wls9-async组件存在反序列化远程命令执行漏洞的安全公告,” 17 4 2019. [Online]. Available: https://www.cnvd.org.cn/webinfo/show/4989.

[37] Oracle, “Oracle Security Alert Advisory - CVE-2019-2725,” 26 4 2019. [Online]. Available: https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html.

[38] KnownSec 404, “[KnownSec 404 Team] Oracle WebLogic Deserialization RCE Vulnerability (0day) Alert Again (CVE-2019‑2725 patch bypassed!!!),” 16 6 2019. [Online]. Available: https://medium.com/@knownsec404team/knownsec-404-team-alert-again-cve-2019-2725-patch-bypassed-32a6a7b7ca15.

[39] Oracle, “Oracle Security Alert Advisory - CVE-2019-2729,” 18 6 2019. [Online]. Available: https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2729-5570780.html.

[40] “Oracle WebLogic Serverの脆弱性（CVE-2019-2725）を狙う攻撃の観測,” 10 5 2019. [Online]. Available: https://wizsafe.iij.ad.jp/2019/05/658/.

[41] NTTデータ先端技術株式会社, “Oracle WebLogic Serverに含まれるリモートコード実行に関する脆弱性（CVE-2019-2725）についての検証レポート,” 9 5 2019. [Online]. Available: http://www.intellilink.co.jp/article/vulner/190509.html.

[42] Microsoft, “CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability,” 14 5 2019. [Online]. Available: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0708.

[43] Microsoft, “Prevent a worm by updating Remote Desktop Services (CVE-2019-0708),” 14 5 2019. [Online]. Available: https://msrc-blog.microsoft.com/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/.

[44] Microsoft, “Customer guidance for CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability: May 14, 2019,” 14 5 2019. [Online]. Available: https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708.

[45] Errata Security, “Almost One Million Vulnerable to BlueKeep Vuln (CVE-2019-0708),” 28 5 2019. [Online]. Available: https://blog.erratasec.com/2019/05/almost-one-million-vulnerable-to.html#.XTBJy-j7RhE.

[46] Microsoft, “A Reminder to Update Your Systems to Prevent a Worm,” 30 5 2019. [Online]. Available: https://msrc-blog.microsoft.com/2019/05/30/a-reminder-to-update-your-systems-to-prevent-a-worm/.

[47] NSA, “NSA Cybersecurity Advisory: Patch Remote Desktop Services on Legacy Versions of Windows,” 4 6 2019. [Online]. Available: https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1865726/nsa-cybersecurity-advisory-patch-remote-desktop-services-on-legacy-versions-of/.

[48] Morphus Labs, “GoldBrute Botnet Brute Forcing 1.5 Million RDP Servers,” 7 6 2019. [Online]. Available: https://morphuslabs.com/goldbrute-botnet-brute-forcing-1-5-million-rdp-servers-371f219ec37d.

[49] CISA, “Alert (AA19-168A) Microsoft Operating Systems BlueKeep Vulnerability,” 17 6 2019. [Online]. Available: https://www.us-cert.gov/ncas/alerts/AA19-168A.

[50] 警察庁, “リモートデスクトップサービスを標的としたアクセスの増加等について,” 21 6 2019. [Online]. Available: http://www.npa.go.jp/cyberpolice/important/2019/201906211.html.

[51] Microsoft, “CVE-2019-0859 | Win32k Elevation of Privilege Vulnerability,” 9 4 2019. [Online]. Available: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0859.

[52] Microsoft, “CVE-2019-0803 | Win32k Elevation of Privilege Vulnerability,” 9 4 2019. [Online]. Available: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0803.

[53] NCSC, “NCSC advice following WhatsApp vulnerability,” 14 5 2019. [Online]. Available: https://www.ncsc.gov.uk/guidance/whatsapp-vulnerability.

[54] Zscaler, “Microsoft vulnerability: Source code published for three zero-day vulnerabilities in Windows,” 24 5 2019. [Online]. Available: https://www.zscaler.com/blogs/research/three-zero-day-microsoft-windows-vulnerabilities.

[55] Filippo Cavallarin, “MacOS X GateKeeper Bypass,” 24 5 2019. [Online]. Available: https://www.fcvl.net/vulnerabilities/macosx-gatekeeper-bypass.

[56] Forbes, “Warning: Google Researcher Drops Windows 10 Zero-Day Security Bomb,” 12 6 2019. [Online]. Available: https://www.forbes.com/sites/daveywinder/2019/06/12/warning-windows-10-crypto-vulnerability-outed-by-google-researcher-before-microsoft-can-fix-it/#28019f052fd6.

[57] Mozilla, “Mozilla Foundation Security Advisory 2019-18,” 18 6 2019. [Online]. Available: https://www.mozilla.org/en-US/security/advisories/mfsa2019-18/.

[58] Microsoft, “Analysis of a targeted attack exploiting the WinRAR CVE-2018-20250 vulnerability,” 10 4 2019. [Online]. Available: https://www.microsoft.com/security/blog/2019/04/10/analysis-of-a-targeted-attack-exploiting-the-winrar-cve-2018-20250-vulnerability/.

[59] matrix, “We have discovered and addressed a security breach. (Updated 2019-04-12),” 12 4 2019. [Online]. Available: https://matrix.org/blog/2019/04/11/we-have-discovered-and-addressed-a-security-breach-updated-2019-04-12.

[60] Sucuri, “ThinkPHP 5.x Remote Code Execution,” 17 4 2019. [Online]. Available: https://blog.sucuri.net/2019/04/thinkphp-5-x-remote-code-execution.html.

[61] Canadian Centre for Cyber Security, “China Chopper Malware affecting SharePoint Servers,” 23 4 2019. [Online]. Available: https://cyber.gc.ca/en/alerts/china-chopper-malware-affecting-sharepoint-servers.

[62] ZDNet, “Microsoft SharePoint servers are under attack,” 10 5 2019. [Online]. Available: https://www.zdnet.com/article/microsoft-sharepoint-servers-are-under-attack/.

[63] TrendMicro, “CVE-2019-3396 Redux: Confluence Vulnerability Exploited to Deliver Cryptocurrency Miner With Rootkit,” 7 5 2019. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-3396-redux-confluence-vulnerability-exploited-to-deliver-cryptocurrency-miner-with-rootkit/.

[64] ITmedia, “Officeの既知の脆弱性を悪用した攻撃が活発化、不正なメールに注意呼び掛け――Microsoft,” 11 6 2019. [Online]. Available: https://www.itmedia.co.jp/enterprise/articles/1906/11/news065.html.

[65] Proofpoint, “Proofpoint Q1 2019 Threat Report: Emotet carries the quarter with consistent high-volume campaigns,” 28 5 2019. [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/proofpoint-q1-2019-threat-report-emotet-carries-quarter-consistent-high-volume.

[66] ZDNet, “Emotet hijacks email conversation threads to insert links to malware,” 11 4 2019. [Online]. Available: https://www.zdnet.com/article/emotet-hijacks-email-conversation-threads-to-insert-links-to-malware/#ftag=RSSbaffb68.

[67] TrendMicro, “Emotet Adds New Evasion Techn,” 25 4 2019. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-adds-new-evasion-technique-and-uses-connected-devices-as-proxy-cc-servers/.

[68] StateScoop, “In Albany ransomware attack, officials say information was not compromised,” 11 4 2019. [Online]. Available: https://statescoop.com/in-albany-ransomware-attack-officials-say-information-was-not-compromised/.

[69] KnowBe4, “County Line Ransomware Fever,” 17 4 2019. [Online]. Available: https://blog.knowbe4.com/county-line-ransomware-fever.

[70] REUTERS, “Bayer contains cyber attack it says bore Chinese hallmarks,” 4 4 2019. [Online]. Available: https://www.reuters.com/article/us-bayer-cyber/bayer-contains-cyber-attack-it-says-bore-chinese-hallmarks-idUSKCN1RG0NN.

[71] Security Next, “メール管理システムがランサムウェア感染 - 神大,” 10 5 2019. [Online]. Available: http://www.security-next.com/104620.

[72] Security Affairs, “Stuart City is the new victim of the Ryuk Ransomware,” 24 4 2019. [Online]. Available: https://securityaffairs.co/wordpress/84439/malware/ryuk-ransomware-stuart-city.html.

[73] “Potter County officials’ computers remain dark after viruses hit,” 22 4 2019. [Online]. Available: https://www.newschannel10.com/2019/04/23/potter-county-officials-computers-remain-dark-after-viruses-hit/.

[74] Security Affairs, “The special-purpose vehicle maker Aebi Schmidt was hit by a malware attack that disrupted some of its operations.,” 26 4 2019. [Online]. Available: https://securityaffairs.co/wordpress/84501/malware/aebi-schmidt-ransomware.html.

[75] BBC, “Baltimore government held hostage by hackers' ransomware,” 23 5 2019. [Online]. Available: https://www.bbc.com/news/world-us-canada-48371476.

[76] 長崎新聞, “佐世保共済病院　患者受け入れ再開　新規と救急　システム障害復旧,” 4 6 2019. [Online]. Available: https://this.kiji.is/508439813399725153.

[77] SECURITY WEEK, “Malware Found on PoS Systems at Checkers and Rally's Restaurants,” 30 5 2019. [Online]. Available: https://www.securityweek.com/malware-found-pos-systems-checkers-and-rallys-restaurants.

[78] ZDNet, “Florida city pays $600,000 to ransomware gang to have its data back,” 19 6 2019. [Online]. Available: https://www.zdnet.com/article/florida-city-pays-600000-to-ransomware-gang-to-have-its-data-back/.

[79] SECURITY WEEK, “Aircraft Parts Maker ASCO Severely Hit by Ransomware,” 13 6 2019. [Online]. Available: https://www.securityweek.com/aircraft-parts-maker-asco-severely-hit-ransomware.

[80] ZDNet, “Second Florida city pays giant ransom to ransomware gang in a week,” 26 4 2019. [Online]. Available: https://www.zdnet.com/article/second-florida-city-pays-giant-ransom-to-ransomware-gang-in-a-week/.

[81] 内閣サイバーセキュリティセンター（NISC）, “サイバーセキュリティ基本法の一部を改正する法律の施行及び 同法に基づくサイバーセキュリティ協議会の組織について,” 内閣サイバーセキュリティセンター（NISC）, 1 4 2019. [Online]. Available: https://www.nisc.go.jp/press/pdf/kyogikai.pdf.

[82] “「電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第1版)」（案）についての意見募集の結果及びガイドラインの公表,” Ministry of Internal Affairs and Communications, 22 4 2019. [Online]. Available: http://www.soumu.go.jp/menu_news/s-news/01kiban05_02000179.html.

[83] National Cyber Security Centre, “Future-proof TLS configuration using the updated TLS guidelines from NCSC,” National Cyber Security Centre, 23 4 2019. [Online]. Available: https://english.ncsc.nl/latest/news/2019/juli/01/future-proof-tls-configuration.

[84] the Department of Homeland Security, “Binding Operational Directive 19-02,” the Department of Homeland Security, 29 4 2019. [Online]. Available: https://cyber.dhs.gov/bod/19-02/.

[85] 一般社団法人共同通信社, “政府、反撃用ウイルス初保有へ,” 一般社団法人共同通信社, 30 4 2019. [Online]. Available: https://this.kiji.is/495701484642698337.

[86] BBC, “Plan to secure internet of things with new law,” BBC, 1 5 2019. [Online]. Available: https://www.bbc.com/news/technology-48106582.

[87] The White House, “Executive Order on America’s Cybersecurity Workforce,” The White House, 2 5 2019. [Online]. Available: https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/.

[88] JIJI PRESS LTD., “インフラ事業者に対策義務付け＝サイバー攻撃、司令塔を新設－自民提言,” JIJI PRESS LTD., 14 5 2019. [Online]. Available: https://www.jiji.com/jc/article?k=2019051401171&g=pol.

[89] IPA, Japan, “入退管理システムにおける情報セキュリティ対策要件チェックリスト,” IPA, Japan, 20 5 2019. [Online]. Available: https://www.ipa.go.jp/security/jisec/choutatsu/ecs/index.html.

[90] Council of Anti-Phishing Japan, “資料公開: フィッシング対策ガイドラインの改訂のお知らせ,” Council of Anti-Phishing Japan, 29 5 2019. [Online]. Available: https://www.antiphishing.jp/news/info/guideline2019.html.

[91] National Institute of Standards and Technology, “Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF),” National Institute of Standards and Technology, 11 6 2019. [Online]. Available: https://csrc.nist.gov/publications/detail/white-paper/2019/06/11/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft.

[92] Ministry of Internal Affairs and Communications, “マルウェアに感染しているIoT機器の利用者に対する注意喚起の実施,” Ministry of Internal Affairs and Communications, 14 6 2019. [Online]. Available: http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00025.html.

[93] National Institute of Standards and Technology, “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks,” National Institute of Standards and Technology, 25 6 2019. [Online]. Available: https://www.nist.gov/publications/considerations-managing-internet-things-iot-cybersecurity-and-privacy-risks.

[94] “All Information (Except Text) for S.1084 - Deceptive Experiences To Online Users Reduction Act,” 9 4 2019. [Online]. Available: https://www.congress.gov/bill/116th-congress/senate-bill/1084/all-info.

[95] “HB 1071 - 2019-20,” 6 8 2019. [Online]. Available: https://app.leg.wa.gov/billsummary?BillNumber=1071&Initiative=false&Year=2019.

[96] D. Palmer, “You’ve been hacked, now what? How the UK’s cybersecurity and privacy watchdogs deal with incidents,” CBS Interactive, 25 4 2019. [Online]. Available: https://www.zdnet.com/article/youve-been-hacked-now-what-how-the-uks-cybersecurity-and-privacy-watchdogs-deal-with-incidents/.

[97] “Letter from Sir Jonathan Thompson to HMRC’s Data Protection Officer,” 3 5 2019. [Online]. Available: https://www.gov.uk/government/publications/letter-from-sir-jonathan-thompson-to-hmrcs-data-protection-officer.

[98] Big Brother Watch, “HMRC takes 5 million taxpayers’ Voice IDs without consent,” Big Brother Watch, 25 6 2018. [Online]. Available: https://bigbrotherwatch.org.uk/all-media/hmrc-takes-5-million-taxpayers-voice-ids-without-consent/.

[99] 忠. 玄, “政府会合が「情報銀行」の標準化など提言、GAFA対抗の「日本モデル」目指す,” Nikkei Business Publications, Inc, 21 5 2019. [Online]. Available: https://tech.nikkeibp.co.jp/atcl/nxt/news/18/05039/.

[100] The Data Protection Commission, “Data Protection Commission opens statutory inquiry into Google Ireland Limited,” The Data Protection Commission, 22 5 2019. [Online]. Available: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-google-ireland-limited.

[101] State of Maine, “An Act To Protect the Privacy of Online Customer Information,” State of Maine, 30 5 2019. [Online]. Available: http://legislature.maine.gov/LawMakerWeb/summary.asp?ID=280072014.

[102] The New York State Senate, “senate Bill S5575B,” The New York State Senate, 25 7 2918. [Online]. Available: https://www.nysenate.gov/legislation/bills/2019/s5575.

[103] BINANCE, “Binance Security Breach Update,” 9 8 2019. [Online]. Available: https://www.binance.com/en/support/articles/360028031711.

[104] Cnet, “US mayors resolve not to pay hackers over ransomware attacks,” 12 7 2019. [Online]. Available: https://www.cnet.com/news/us-mayors-adopt-resolution-to-not-pay-hackers-over-ransomware-attacks/.

[105] Japan Registry Services Co., Ltd., “JPRS用語辞典｜レジストリ,” Japan Registry Services Co., Ltd., [Online]. Available: https://jprs.jp/glossary/index.php?ID=0102.

[106] Japan Registry Services Co., Ltd., “JPRS用語辞典｜レジストラ,” Japan Registry Services Co., Ltd., [Online]. Available: https://jprs.jp/glossary/index.php?ID=0101.

NTT DATA
Trusted Global Innovator

August 29, 2019

NTT DATA Corporation
NTTDATA-CERT, Information Security Office, Security Engineering Department
Hisamichi Ohtani / Yoshinori Kobayashi / Masao Oishi / Daisuke Yamashita
nttdata-cert@kits.nttdata.co.jp